Claims

I CLAIM:

1. An apparatus for handling SSL traffic comprising an SSL proxy operable to receive a plurality of packets each including an encrypted portion, the SSL proxy operable to buffer the packets until a predetermined number of packets are received, the SSL proxy further operable to decrypt the encrypted portion of each received packet and forward the decrypted packets to a predetermined destination.

2. The apparatus of Claim 1, wherein the SSL proxy includes a database operable to track information regarding a type of encryption scheme used to encrypt the encrypted portion.

3. The apparatus of Claim 1, wherein the encrypted portion of the packets are decrypted when received and the SSL proxy buffers the received packets out of order.

4. The apparatus of Claim 1, wherein the SSL proxy tracks a message authentication code used to authenticate a message.

5. The apparatus of Claim 1, wherein the packets are sent by a client computer and received by a server computer.

6. The apparatus of Claim 5, wherein the SSL proxy is operable to receive unencrypted data from the server computer, encrypt the unencrypted data, and send the encrypted data to a client computer.

7. The apparatus of Claim 1, wherein the SSL proxy performs encryption and decryption on packets using a single end-to-end TCP connection between a client computer and a server.

8. A system for handling SSL traffic comprising:

a client computer operable to initiate an SSL session and to send packets with encrypted payloads;

a server computer operable to support communications with the client computer; and

a SSL proxy coupling the client computer and the server computer and operable to decrypt the encrypted payloads of each packet and forward the decrypted packets to the server computer.

9. The system of Claim 8, wherein the SSL proxy includes a database operable to track information regarding a type of encryption scheme used to encrypt the encrypted payloads.

10. The system of Claim 8, wherein the packets are decrypted when received by the SSL proxy and the SSL proxy buffers the received packets out of order.

11. The apparatus of Claim 8, wherein the SSL proxy tracks a message authentication code used to authenticate a message.

12. The system of Claim 8, wherein the SSL proxy is operable to encrypt packets sent from the server computer to the client computer.

13. The system of Claim 8, wherein a single end-to-end TCP connection exists between the client computer and the server computer.

14. The system of Claim 8, wherein the SSL proxy buffers the packets until a predetermined number of packets arrive, then decrypts packets, and forward the decrypted packets to the server.

15. A method for processing SSL packets comprising:

initializing an SSL session between a client computer and a SSL proxy;

receiving a packet including an encrypted portion at the SSL proxy;

determining if the received packet is a SSL packet;

placing the received packet in a hold queue;

checking the hold queue for a complete set of packets;

decrypting the encrypted portion of each packet once the complete set of packets are received; and

outputting the decrypted packets to a server computer.

16. The method of Claim 15, wherein a message authentication code is checked to verify authenticity of the packet set.

17. The method of Claim 15, wherein non SSL packets are sent directly to the server.

18. The method of Claim 15, wherein the step of placing the packets in a hold queue comprises:

placing packets received out of order in a queue;

decrypting packets received in order and forwarding the decrypted packets to a server computer;

checking the hold queue to determine if the packet in the queue is next in sequence;

releasing the packet from the hold queue if the packet in hold queue is the next in sequence; and

getting a new packet if the packet in the hold queue is not the next in sequence.

19. The method of Claim 15, wherein the step of initializing further comprises initializing a single end-to-end TCP connection between the client computer and the server computer.

20. The method of Claim 15, further comprising:

receiving packets with unencrypted data at a SSL proxy from the server computer;

encrypting the packets at the SSL proxy; and

sending the encrypted packets to the client computer.

21. An apparatus for decrypting network data traffic comprising a proxy operable to:

(i) receive packets addressed to a server computer, the packets including an encrypted portion, a destination address, and a source address;

(ii) decrypt the encrypted portions of the received packets; and

(iii) send the decrypted portions to a server computer without altering the destination or source address of the received packets.

22. The apparatus of Claim 21, wherein the proxy is further operable to:

(i) receive packets addressed to a client computer, the packets including an unencrypted portion, a destination address, and a source address;

(ii) encrypt the unencrypted portion of the received packets; and

(iii) send the encrypted packets to the client computer without altering the destination or source address of the packets.